

Operational Interpretation of the G -asymmetry for Abelian Groups

Michael Skotiniotis¹ and Gilad Gour^{1,2}

¹*Institute for Quantum Information Science, University of Calgary,
2500 University Drive NW, Calgary AB, T2L 1N1, Canada*

²*Department of Mathematics and Statistics, University of Calgary,
2500 University Drive NW Calgary, Alberta, T2N 1N4, Canada*

(Dated: February 16, 2012)

We determine the quantum states and measurements that optimize the accessible information in a reference frame alignment protocol associated with the groups $U(1)$, corresponding to a phase reference, and \mathbb{Z}_M , the cyclic group of M elements. Our result provides an operational interpretation for the G -asymmetry which is information-theoretic and which was thus far lacking. In particular, we show that in the limit of many copies of the bounded-size quantum reference frame, the accessible information approaches the Holevo bound. This implies that the rate of alignment of reference frames, measured by the (linearized) accessible information per system, is equal to the regularized, linearized G -asymmetry. The latter quantity is equal to the variance in the case where $G = U(1)$. Quite surprisingly, for the case where $G = \mathbb{Z}_M$ and $M \geq 4$, it is equal to a quantity that is not additive in general, but instead can be superadditive under tensor product of two distinct bounded-size reference frames. This remarkable phenomenon is purely quantum and has no classical analog.

I. INTRODUCTION

States and transformations of systems are defined relative to an external frame of reference. If the alignment of two distant reference frames deteriorates with time, or if the state one possesses was prepared according to some reference frame one does not have access to, super-selection rules are imposed on the kind of states that can be prepared and the type of operations that can be implemented [1]. For example, lacking a Cartesian frame of reference associated with the rotation group, $SO(3)$, implies that one can only prepare rotationally invariant states and perform rotationally invariant operations. The lack of a reference frame can be alleviated (at least partially) if a party is provided with a bounded-size quantum reference frame [2]; i.e. a non-invariant ($SO(3)$ -asymmetric) state, such as the state of a particle with integer spin pointing in some known direction [3]. In the general case where the lack of a requisite reference frame is associated with a finite or compact Lie group G , such G -asymmetric states are considered *resources*. They are measured by functions, called “frameness monotones” [4] or simply asymmetry measures [5, 6], that do not increase under the set of allowable (i.e. G -invariant) quantum operations.

There are several measures in the literature that quantify asymmetry for particular groups [4], or in particular dimensions [7]. However, there exists one measure, the G -asymmetry [8], that is defined for all groups and all dimensions. The G -asymmetry of a state $\rho \in \mathcal{B}(\mathcal{H}_d)$, a bounded, positive semi-definite operator acting on a d -dimensional Hilbert space \mathcal{H}_d , is defined as

$$A_G(\rho) := S(\mathcal{G}[\rho]) - S(\rho), \quad (1)$$

where $\mathcal{G}(\cdot) \equiv \int dg T(g)(\cdot)T(g)^\dagger$ is the G -twirling operation, with the integral performed over the Haar measure dg , T a representation of G on the Hilbert space \mathcal{H}_d , and S the von Neumann entropy. For the case of finite groups,

the integral in the G -twirling operation is replaced by a sum, and the invariant Haar measure is given by $1/|G|$, where $|G|$ is the order of the group. The G -asymmetry was shown to be equal to the relative entropy of frameness [6], the latter being analogous to the relative entropy of entanglement [9].

In this work we consider the case where $G = \mathbb{Z}_M$, the cyclic group of M elements, and the case where $G = U(1)$ associated with the important case of photon number super-selection. For these cases we provide an operational interpretation for the G -asymmetry that is information theoretic, different than the interpretation in [8] of the G -asymmetry as extractable mechanical work. In particular, we find the strategy for aligning a pair of reference frames associated with G that optimizes the amount of accessible information between the true relation, $g \in G$, of the two reference frames and the estimated relation, $g' \in G$, obtained by measurement. Our approach is different from previous work on reference frame alignment protocols where the success of the protocol was quantified by maximizing an average cost, such as the fidelity or the maximum likelihood of a correct guess [3, 10–16] (for a review of these protocols see [17]). More precisely, we show that asymptotically the amount of accessible information is equal to the G -asymmetry. As the accessible information is upper bounded by the Holevo quantity [18], our result also implies that for a reference frame alignment protocol associated with $G = \mathbb{Z}_M$ and $G = U(1)$, the Holevo bound is asymptotically achievable.

This paper is organized as follows. In Sec. II we review the resource theory of reference frames and the connection between the G -asymmetry, the relative entropy of frameness, and the Holevo bound. In Sec. III we present our main results, and determine the asymptotic rate of transmission of information in a phase alignment protocol (Sec. III A) [17], and in a reference frame alignment protocol associated with $G = \mathbb{Z}_M$ (Sec. III B). In Sec. IV

we discuss the additivity and superadditivity of the linearized, regularized G asymmetry for both the $U(1)$ and \mathbb{Z}_M cases. We end in Sec. V with summary and conclusions.

II. RELATIVE ENTROPY OF FRAMENESS, THE HOLEVO BOUND, AND THE ALIGNMENT RATE

Suppose two parties, Alice and Bob, wish to align their reference frames associated with some group G . Let $T : G \rightarrow \mathcal{H}_d$ be the unitary representation of G on a d -dimensional Hilbert space \mathcal{H}_d . Alice prepares a system in a state $|\psi\rangle \in \mathcal{H}_d$ and sends this system to Bob. Assuming that Bob has complete ignorance as to which element $g \in G$ relates his reference frame to Alice's, Bob's description of the state of the system sent to him by Alice is given by the ensemble $\{dg, T(g)|\psi\rangle\}$, where dg is the Haar measure of the group G , or equivalently by the G -twirling of $|\psi\rangle$.

Alternatively, we can think of the above scenario in the following way. We can assume that Alice and Bob share a common frame of reference, but instead of sending the state $|\psi\rangle$, Alice sends Bob a state $T(g)|\psi\rangle$ picked from the ensemble $\{dg, T(g)|\psi\rangle\}$. Bob's task is to determine g . In this view it is natural to quantify Bob's success in determining g by the accessible information.

Let X be the random variable consisting of the elements of G with uniform probability distribution given by the Haar measure. Alice sends classical information to Bob by preparing a system in the state $\rho(X) = T(X)\rho T(X)^\dagger$, where later we will assume that $\rho = |\psi\rangle\langle\psi|$ is a pure state. Bob performs a positive operator valued measure (POVM) $\{E_y\}$, and obtains outcome y with probability p_y . Let Y denote the random variable associated with Bob's measurement outcome. The *accessible information*, $I^{(1)}(X : Y)$, for a single system is defined as the maximum amount of mutual information between random variables X and Y , where the maximization is performed over all of Bob's possible POVMs. An upper bound for the accessible information is the Holevo quantity [18] which in the case of continuous groups is given by

$$\chi^{(1)} = S(\mathcal{G}[\rho]) - \int dg S(T(g)\rho T(g)^\dagger), \quad (2)$$

where $S(\cdot)$ is the von Neumann entropy. If G is a finite group, then the integral in Eq. (2) is replaced by a sum, and $p_g = 1/|G|$. Since for any unitary transformation U , $S(U\rho U^\dagger) = S(\rho)$, the G -asymmetry given by Eq. (1) is equal to the Holevo quantity and thus is an upper bound for the accessible information [6]. For N copies of a system prepared in the state ρ , the accessible information, $I^{(N)}(X : Y)$, is upper bounded by $\chi^{(N)}$, which is equal to the G -asymmetry, $A_G(\rho^{\otimes N})$, of the state $\rho^{\otimes N}$.

The G -asymmetry is also related to the relative en-

tropy of frameness defined as

$$\min_{\sigma \in \mathcal{I}} S(\rho||\sigma), \quad (3)$$

where $S(\rho||\sigma) = -S(\rho) - \text{tr}(\rho \log \sigma)$, and $\mathcal{I} \equiv \{\sigma | \mathcal{G}[\sigma] = \sigma \in \mathcal{B}(\mathcal{H}_d)\}$ is the set of invariant states [6]. Due to the invariance of the Haar measure, the G -twirling operation \mathcal{G} , is idempotent, $\mathcal{G} \circ \mathcal{G} = \mathcal{G}$, and unital, $\mathcal{G}[I] = I$. For such a quantum operation it was shown in [6] that the minimum relative entropy distance between an arbitrary state $\rho \in \mathcal{B}(\mathcal{H})$ and a state $\sigma \in \mathcal{I}$ satisfies

$$\min_{\sigma \in \mathcal{I}} S(\rho||\sigma) = S(\mathcal{G}[\rho]) - S(\rho). \quad (4)$$

Thus, the G -asymmetry is equal to the relative entropy of frameness.

In entanglement theory, the regularized relative entropy of entanglement has an operational interpretation. It quantifies the rate of interconversion between states in a reversible theory of entanglement [19]. One can therefore expect that the relative entropy of frameness would have an operational interpretation similar to that of the relative entropy of entanglement. However, it was shown in [6] that the regularized relative entropy of frameness is zero on all states;

$$\lim_{N \rightarrow \infty} \frac{A_G(\rho^{\otimes N})}{N} = 0.$$

This is because the relative entropy of frameness is not an extensive quantity, i.e. it does not scale linearly with the number of systems N , unlike the relative entropy of entanglement.

For this reason, and following [6], we introduce here the *linearization function* \mathcal{L} . The linearization function $\mathcal{L} : \mathbb{R} \rightarrow \mathbb{R}$ is a monotonically increasing function that linearizes $A_G(\rho^{\otimes N})$; that is, \mathcal{L} is chosen such that $\mathcal{L}(A_G(\rho^{\otimes N})) \propto N$ in the limit of large N . With such a choice for \mathcal{L} , we can rescale both the accessible information and the G -asymmetry so that they become extensive quantities. We therefore define the *regularized*, linearized G -asymmetry as follows:

$$A_G^{(reg)}(\psi) \equiv \lim_{N \rightarrow \infty} \frac{\mathcal{L}(A_G(|\psi\rangle\langle\psi|^{\otimes N}))}{N}. \quad (5)$$

We will show in the next section that the above quantity has an operational interpretation for $G = \mathbb{Z}_M$ or $G = U(1)$. It measures the rate, $R_G(\psi)$, at which many copies of a bounded-size quantum reference frame, $|\psi\rangle$, elevate the restrictions induced by the lack of a shared reference frame. We now give its precise definition.

Definition 1 The alignment rate of a state $|\psi\rangle$ is defined by

$$R_G(\psi) \equiv \lim_{N \rightarrow \infty} \frac{\mathcal{L}(I^{(N)}(X : Y))}{N}$$

That is, $R_G(\psi)$, measures the rate at which Bob learns about the orientation of Alice's reference frame from

many copies of a bounded-size quantum reference frame, $|\psi\rangle$. By definition, $R_G(\psi)$ is a deterministic frameness monotone [4] (i.e. does not increase under deterministic G -invariant operations). Furthermore, since \mathcal{L} is a monotonic function, the Holevo bound implies that $R_G(\psi)$ is bounded above by $A_G^{(reg)}(\psi)$. In the next section we show that in fact $R_G(\psi) = A_G^{(reg)}(\psi)$ for the case where $G = U(1)$ (Sec. III A), associated with the case where two parties lack a common phase reference, and for the case where the reference frame is associated with the finite cyclic group of M elements, \mathbb{Z}_M (Sec. III B).

III. OPTIMAL RATE FOR ALIGNMENT OF REFERENCE FRAMES

In this section we determine the optimal alignment rate for the cases where Alice and Bob lack a shared frame of reference associated with $G = U(1)$ and $G = \mathbb{Z}_M$.

A. Phase reference

We begin by considering two parties, Alice and Bob, who share an ideal quantum channel but lack a shared phase reference as discussed in Sec. II. The relevant group of transformations associated with a phase reference is $U(1)$, the group of real numbers modulo 2π . Physically, Alice and Bob lack a shared phase reference if their local oscillators have an unknown relative phase, i.e. they are not phase locked. The unitary representation, T , describing a phase shift $\theta \in U(1)$ is given by $T(\theta) = e^{i\theta\hat{N}}$, where \hat{N} is the number operator. If Alice and Bob have complete ignorance as to the relative phase between their respective local oscillators, then any state $\rho \in \mathcal{B}(\mathcal{H})$ prepared by Alice is described as $\mathcal{G}[\rho]$ by Bob.

As the number operator is unbounded (from above), T acts on an infinite dimensional Hilbert space, \mathcal{H} . Using Schur's lemmas [20], the representation T can be decomposed into the one-dimensional irreducible representations (irreps), $T^{(n)}(\theta) = e^{i\theta n}$ of $U(1)$,

$$T(\theta) = \bigoplus_{n=0}^{\infty} \alpha_n T^{(n)}(\theta), \quad (6)$$

where the irrep label n represents the total photon number, and α_n is the multiplicity of irrep $T^{(n)}$.

Without a shared phase reference Alice faces a restriction on the type of states she can prepare with respect to Bob's phase reference. That is, the lack of a shared phase reference with Bob, imposes a photon number super-selection rule in which superpositions of photon number eigenstates cannot be prepared by Alice [17]. Consequently, it is convenient to write the total Hilbert space, \mathcal{H} , as

$$\mathcal{H} = \bigoplus_{n=0}^{\infty} \mathcal{H}^{(n)} = \bigoplus_{n=0}^{\infty} \mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}, \quad (7)$$

where $\mathcal{M}^{(n)}$ carries the irrep $T^{(n)}$, and $\mathcal{N}^{(n)}$ carries the trivial representation of $U(1)$.

In addition to preparation of states, a photon number super-selection rule also imposes restrictions on the types of operations Alice can perform (relative to Bob's reference frame). More precisely, Alice is restricted to $U(1)$ -invariant operations, which were shown in [4] to be of two types: shifts in the total photon number (by adding or removing photons), and changes in the relative amplitudes of different photon number states. In particular, the set of $U(1)$ -invariant *reversible* transformations consists of all unitary matrices that commute with the number operator and shifts (in photon number).

Thus, any qudit $|\psi\rangle \in \mathcal{H}$, can be brought by $U(1)$ -invariant unitary transformations (and shifts), to a standard form

$$|\psi\rangle = \sum_{n=0}^{d-1} \sqrt{p_n} |n\rangle, \quad (8)$$

where $\sum_n p_n = 1$, and $|n\rangle \equiv |n, \alpha = 1\rangle$ is a state in $\mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}$ chosen to be the standard one. This is because under a photon number super-selection rule all states $|n, \alpha\rangle \in \mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}$, for a given total photon number n , are equivalent up to $U(1)$ -invariant unitary transformations. Hence, we can pick any pure state, say $|n, \alpha = 1\rangle \in \mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}$, as our standard one.

In the phase alignment protocol we consider here, Alice sends N copies of a qudit prepared in the state $|\psi\rangle$ of Eq. (8) to Bob. The state $|\psi\rangle^{\otimes N}$ is a superposition of the *tensor product basis* $\{|x_1 \dots x_N\rangle, x_1, \dots, x_N \in (0, \dots, d-1)\}$. Each such state can be written in terms of the total photon number, n , and its multiplicity α . That is, $|n, \alpha\rangle \equiv |x_1 \dots x_N\rangle$ and $\alpha = 1, \dots, l_n$, where l_n denotes the number of orthonormal states with the same photon number n . In the basis $|n, \alpha\rangle$, the state $|\psi\rangle^{\otimes N}$ can be written as

$$|\psi\rangle^{\otimes N} = \sum_{n=0}^{N(d-1)} \sum_{\alpha=1}^{l_n} \sqrt{c_{n,\alpha}} |n, \alpha\rangle, \quad (9)$$

where $c_{n,\alpha}$ are of the form $c_{n,\alpha} = \prod_{j=0}^{d-1} p_j^{r_j}$, and r_j are positive integers (corresponding to the number of times $x_j \in (0, \dots, d-1)$ appears in $|n, \alpha\rangle$) satisfying $\sum_j r_j = N$ and $\sum_j j r_j = n$. Moreover, by $U(1)$ -invariant unitary operations we can transform

$$\frac{\sum_{\alpha} \sqrt{c_{n,\alpha}} |n, \alpha\rangle}{\sqrt{\sum_{\alpha} c_{n,\alpha}}}, \quad (10)$$

to the standard state $|n\rangle \in \mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}$. This transformation brings $|\psi\rangle^{\otimes N}$ to the form

$$|\psi\rangle^{\otimes N} = \sum_{n=0}^{N(d-1)} \sqrt{c_n} |n\rangle, \quad (11)$$

where (see [4, 21])

$$c_n = \sum \binom{N}{r_0 \dots r_{d-1}} p_0^{r_0} \dots p_{d-1}^{r_{d-1}} \quad (12)$$

are the multinomial coefficients that arise from the expansion $(\sum_n \sqrt{p_n} |n\rangle)^{\otimes N}$, where terms giving rise to the same total photon number n are grouped together. We note that the sum in Eq. (12) is taken over all non-negative integers r_j for which $\sum_{j=0}^{d-1} r_j = N$ and $\sum_{j=0}^{d-1} j r_j = n$.

Bob's description of the N qudits sent to him by Alice is given by

$$|\psi(\theta)\rangle^{\otimes N} = (T(\theta) |\psi\rangle)^{\otimes N} = \sum_{n=0}^{N(d-1)} \sqrt{c_n} e^{in\theta} |n\rangle. \quad (13)$$

Due to the lack of a shared phase reference, Bob has complete ignorance about the value of θ . As the superselection rule does not forbid us from performing any unitary on the multiplicity spaces, the state $|\psi(\theta)\rangle^{\otimes N}$ can be embedded in a $(N(d-1)+1)$ -dimensional Hilbert space. This is the key reason why the $U(1)$ -asymmetry is not an extensive quantity. Bob's task is, therefore, to extract information about θ from a state in an $N(d-1)+1$ -dimensional Hilbert space instead of a d^N -dimensional Hilbert space.

Suppose Bob's POVM is given by $\{E_{\theta'}, d\theta'\}$, where $E_{\theta'} \geq 0$ with $\int_0^{2\pi} E_{\theta'} d\theta' = I = \sum_{n=0}^{N(d-1)} |n\rangle\langle n|$. We would like to quantify how much Bob learns about θ from such a measurement. Denote by Θ the random variable associated with the relative phase, θ , between Alice's and Bob's phase references. That is, $\Theta = \theta$ with uniform probability distribution $p_\theta = 1/2\pi$. Denote also by Θ' the random variable associated with Bob's measurement outcome θ' . Then, as discussed in the previous section, the accessible information, $I^{(N)}(\Theta : \Theta')$, satisfies

$$I^{(N)}(\Theta : \Theta') \leq A_{U(1)}(|\psi\rangle\langle\psi|^{\otimes N}). \quad (14)$$

Using Eqs. (1, 13), the right-hand side of Eq. (14) is

$$\begin{aligned} A_{U(1)}(|\psi\rangle\langle\psi|^{\otimes N}) &= S(\mathcal{G}[|\psi\rangle\langle\psi|^{\otimes N}]) - S(|\psi\rangle\langle\psi|^{\otimes N}) \\ &= S\left(\sum_{n=0}^{N(d-1)} c_n |n\rangle\langle n|\right) = H(\{c_n\}), \end{aligned} \quad (15)$$

where $H(\{c_n\})$ is the Shannon entropy of the probability distribution $\{c_n\}$. Consequently, the accessible information per copy of the state $|\psi\rangle \in \mathcal{H}_d$ obeys

$$\frac{I^{(N)}(\Theta : \Theta')}{N} \leq \frac{H(\{c_n\})}{N}. \quad (16)$$

We are interested in determining the accessible information per copy in the limit where the number of copies $N \rightarrow \infty$. However, in this limit the right-hand side of Eq. (16) tends to zero [6]. Indeed, so long as the photon number spectrum is gapless, i.e. $p_n \neq 0$ for $0 < n < d-1$ [21], the probability distribution, $\{c_n\}$, can be approximated, in the limit $N \rightarrow \infty$, with the normal

distribution [22]

$$c_n = \frac{1}{\sqrt{2\pi\sigma_N^2}} \exp\left(-\frac{(n - \mu_N)^2}{2\sigma_N^2}\right) + O\left(\frac{1}{N}\right), \quad (17)$$

where

$$\begin{aligned} \sigma_N^2 &= NV(\psi) \equiv N \left(\sum_{n=0}^{d-1} n^2 p_n - \left(\sum_{n=0}^{d-1} n p_n \right)^2 \right) \\ \mu_N &= N \sum_{n=0}^{d-1} n p_n, \end{aligned} \quad (18)$$

with $V(\psi)$ the variance of the state $|\psi\rangle$. Using Eq. (17) the right-hand side of Eq. (15) reads (see [6] for details)

$$\frac{H(\{c_n\})}{N} = \frac{\frac{1}{2} \log(4\pi NV(\psi)) + O\left(\frac{1}{\sqrt{N}}\right)}{N}. \quad (19)$$

Due to the logarithmic dependence of $H(\{c_n\})$ on N the $U(1)$ -asymmetry is not an extensive quantity, and as a result the limit $N \rightarrow \infty$ of Eq. (19) tends to zero.

Following our discussion in the previous section, we introduce the linearization function, $\mathcal{L}(x) = 2^{2x}$, so that the regularized $U(1)$ -asymmetry is given by

$$A_{U(1)}^{(reg)}(\psi) = \lim_{N \rightarrow \infty} \frac{\mathcal{L}(A_{U(1)}(|\psi\rangle\langle\psi|^{\otimes N}))}{N} = 4\pi V(\psi). \quad (20)$$

Furthermore, as $\mathcal{L}(x) = 2^{2x}$ is a monotonically increasing function, it follows from Eq. (16) that Eq. (20) is an upper bound for the rate of accessible information

$$\frac{\mathcal{L}(I^{(N)}(\Theta : \Theta'))}{N} \leq \frac{\mathcal{L}(A_{U(1)}(|\psi\rangle\langle\psi|^{\otimes N}))}{N}. \quad (21)$$

In the following theorem we show that in the limit $N \rightarrow \infty$, the inequality in Eq. (21) is saturated, meaning that, for $G = U(1)$, the alignment rate as defined in Definition 1 is equal to the regularized, linearized G -asymmetry.

Theorem 1 For $G = U(1)$

$$R_G(\psi) = A_G^{(reg)}(\psi) = 4\pi V(\psi),$$

where, $V(\psi)$ is the variance of the state $|\psi\rangle$.

Proof. Recall that the accessible information is the maximum mutual information, $H(\Theta : \Theta')$, over all possible POVMs. Let Bob's POVM elements be given by $E_{\theta'} = |e_{\theta'}\rangle\langle e_{\theta'}|$, where

$$|e(\theta')\rangle = \frac{1}{\sqrt{2\pi}} \sum_{n=0}^{N(d-1)} e^{in\theta'} |n\rangle. \quad (22)$$

Note that $\int d\theta' E_{\theta'} = I^{(N)}$, where $I^{(N)} = \sum_{n=0}^{N(d-1)} |n\rangle\langle n|$. We remark that the measurement of

Eq. (22) has been shown to optimize the average maximum likelihood [23] and the average fidelity [17]. We will show that in the limit $N \rightarrow \infty$ this measurement also maximizes $H^{(N)}(\Theta : \Theta')$ given by

$$H^{(N)}(\Theta : \Theta') = \int_0^{2\pi} d\theta \int_0^{2\pi} d\theta' p(\theta, \theta') \log \left(\frac{p(\theta, \theta')}{p(\theta') p(\theta)} \right), \quad (23)$$

where the joint probability distribution, $p(\theta, \theta')$ can be calculated using Bayes' rule, $p(\theta, \theta') = p(\theta'|\theta)p(\theta)$. In our case

$$\begin{aligned} p(\theta) &= \frac{1}{2\pi} \\ p(\theta'|\theta) &= \left| \langle e(\theta') | \psi(\theta) \rangle^{\otimes N} \right|^2 \end{aligned} \quad (24)$$

Substituting Eqs. (13, 22) into Eq. (24) gives

$$\begin{aligned} p(\theta'|\theta) &= \frac{1}{2\pi} \sum_{n,m=0}^N \sqrt{c_n c_m} e^{i(m-n)(\theta-\theta')} \\ &= \frac{1}{2\pi} \left| \sum_{m=0}^N \sqrt{c_m} e^{im(\theta-\theta')} \right|^2 \end{aligned} \quad (25)$$

From the equation above we see that $p(\theta'|\theta) = p(\theta|\theta')$. Therefore, the probability that $\Theta' = \theta'$ is given by

$$p(\theta') = \int_0^{2\pi} p(\theta'|\theta)p(\theta)d\theta = \frac{1}{2\pi} \int_0^{2\pi} p(\theta|\theta')d\theta = \frac{1}{2\pi}.$$

Hence, Eq. (23) reduces to

$$H^{(N)}(\Theta : \Theta') = \frac{1}{2\pi} \int_0^{2\pi} d\theta \int_0^{2\pi} d\theta' p(\theta'|\theta) \log(2\pi p(\theta'|\theta)). \quad (26)$$

The expression for the conditional probabilities $p(\theta'|\theta)$ can be greatly simplified as we now show. Note that the sum in Eq. (25) runs over positive integers. In the limit of large N the sum can be approximated by an integral over a continuous variable m . Furthermore, as μ_N is large and positive, the probability distribution corresponding to small photon numbers lies at the tail end of the Gaussian. Using the properties of the error function the lower limit of integration can be extended to negative photon numbers, accumulating a negligible ($O(N^{-1})$) total probability. Making a change of variable, $\phi = \theta - \theta'$, and using Eq. (17), Eq. (25) becomes

$$\begin{aligned} p_\phi \equiv p(\theta|\theta') &= \frac{1}{\sqrt{2\pi\sigma_N^2}} \left| \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{\left(-\frac{(m-\mu_N)^2}{4\sigma_N^2}\right)} e^{im\phi} dm \right|^2 \\ &+ O\left(\frac{1}{\sqrt{N}}\right) \\ &= \sqrt{\frac{2\sigma_N^2}{\pi}} e^{-2\phi^2\sigma_N^2} + O\left(\frac{1}{\sqrt{N}}\right). \end{aligned} \quad (27)$$

Using Eq. (27) and noting that

$$\int_0^{2\pi} d\theta \int_0^{2\pi} d\theta' = \int_{-2\pi}^{2\pi} d\phi \int_\phi^{\phi+2\pi} d\theta, \quad (28)$$

Eq. (26) reduces to

$$\begin{aligned} H^{(N)}(\Theta : \Theta') &= \sqrt{\frac{2\sigma_N^2}{\pi}} \int_{-2\pi}^{2\pi} d\phi e^{-2\phi^2\sigma_N^2} \\ &\times \log \left(\sqrt{8\pi\sigma_N^2} e^{-2\phi^2\sigma_N^2} \right) + O\left(\frac{1}{\sqrt{N}}\right). \end{aligned} \quad (29)$$

We note that the mutual information does not depend on the mean photon number as expected, since the latter can be shifted using $U(1)$ -invariant operations, and therefore cannot carry any phase information.

Using the approximations

$$\begin{aligned} \int_{-2\pi}^{2\pi} d\phi e^{-2\phi^2\sigma_N^2} &= \int_{-\infty}^{\infty} dx e^{-2\sigma_N^2 x^2} + O\left(\frac{1}{N}\right) \\ \int_{-2\pi}^{2\pi} d\phi \phi^2 e^{-2\phi^2\sigma_N^2} &= \int_{-\infty}^{\infty} dx x^2 e^{-2\sigma_N^2 x^2} + O\left(\frac{1}{N}\right), \end{aligned} \quad (30)$$

where the integrals on the right-hand side of Eq. (30) are equal to $\sqrt{\pi/2\sigma_N^2}$, and $1/2\sqrt{\pi/8\sigma_N^6}$, respectively, one obtains, after simple algebra,

$$H^{(N)}(\Theta : \Theta') = \frac{1}{2} \log(4\pi\sigma_N^2) + O\left(\frac{1}{\sqrt{N}}\right). \quad (31)$$

Finally, linearizing the accessible information and taking the limit gives

$$\lim_{N \rightarrow \infty} \frac{\mathcal{L}(I^{(N)}(\Theta : \Theta'))}{N} = \lim_{N \rightarrow \infty} \frac{2 \log(4\pi N V(\psi))}{N} = 4\pi V(\psi). \quad (32)$$

This completes the proof. \square

B. Reference frame associated with \mathbb{Z}_M

We now consider the case where Alice and Bob share an ideal quantum channel but lack a shared reference frame associated with the finite cyclic group of M elements, \mathbb{Z}_M . For example, the case $G = \mathbb{Z}_2$ corresponds to the situation where Alice and Bob lack a reference frame for chirality [4]. Unlike the $U(1)$ -case, we find that in this case the optimal rate for the alignment of reference frames is not proportional to the variance even in the limit $M \rightarrow \infty$. This is not inconsistent with Theorem 1 of the previous subsection since our main assumption here is that $N \gg M$. Therefore, the results obtained in this subsection are completely independent on the previous subsection.

The unitary representation $T(g)$ (with $g \in \mathbb{Z}_M$) acting on the Hilbert space \mathcal{H} can be decomposed into one-dimensional irreps $T^{(k)}$ as

$$T(g) = \bigoplus_{k=0}^{M-1} \alpha_k T^{(k)}(g). \quad (33)$$

where k labels the irreps of \mathbb{Z}_M , and α_k is the multiplicity of irrep $T^{(k)}$. Just as in the $U(1)$ case above the lack of a shared reference frame associated with \mathbb{Z}_M imposes restrictions on the type of states Alice can prepare with respect to Bob's reference frame. In order to describe these restrictions, it is convenient to write the total Hilbert space, \mathcal{H} , as

$$\mathcal{H} = \bigoplus_{k=0}^{M-1} \mathcal{H}^{(k)} = \bigoplus_{k=0}^{M-1} \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}, \quad (34)$$

where $\mathcal{M}^{(k)}$ is the carrier space of $T^{(k)}$, and $\mathcal{N}^{(k)}$ carries the trivial representation of \mathbb{Z}_M . Thus, the lack of a shared reference frame, associated with \mathbb{Z}_M , imposes a super-selection rule in which superpositions of states from different sectors $\mathcal{H}^{(k)}$ cannot be prepared. Note that unlike the $U(1)$ case above, there are a finite number of sectors, $\mathcal{H}^{(k)}$, equal to the order of the group.

In addition to preparation of states, a \mathbb{Z}_M super-selection rule also imposes restrictions on the types of operations Alice can perform (relative to Bob's reference frame). More precisely, Alice is restricted to \mathbb{Z}_M -invariant operations. In the case where Alice and Bob lack a chiral frame of reference (associated with \mathbb{Z}_2) it was shown in [4] that \mathbb{Z}_2 -invariant operations are of two types: shifts in the irrep label k (which in the case of chiral frames corresponds to the bit flip operation, X), and changes in the relative amplitudes of different eigenstates of irrep label k . Similarly, in the case of a \mathbb{Z}_M super-selection rule, the \mathbb{Z}_M -invariant operations consist of shifts (mod M) in the irrep label k , and changes in the relative amplitudes of different eigenstates of irrep label k .

Thus, any qudit $|\psi\rangle \in \mathcal{H}$, can be brought by \mathbb{Z}_M -invariant unitary transformations (and shifts), to a standard form

$$|\psi\rangle = \sum_{k=0}^{M-1} \sqrt{p_k} |k\rangle, \quad (35)$$

where $\sum_k p_k = 1$, and $|k\rangle \equiv |k, \alpha = 1\rangle \in \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$ is a state in $\mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$ chosen to be the standard one. This is because under the \mathbb{Z}_M super-selection rule all states $|k, \alpha\rangle \in \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$, for a given irrep label k , are equivalent up to \mathbb{Z}_M -invariant unitary transformations. Hence, we can pick any pure state, say $|k, \alpha = 1\rangle \in \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$, as our standard one.

In the reference frame alignment protocol we consider here, where the reference frame is associated with \mathbb{Z}_M , Alice sends N copies of a qudit prepared in the state $|\psi\rangle$ of Eq. (35) to Bob. The state $|\psi\rangle^{\otimes N}$ is a superposition of the tensor product basis $\{|x_1 \dots x_N\rangle, x_1, \dots, x_N \in (0, \dots, d-1)\}$. Each such state can be written in terms of the irrep label k , and its multiplicity α . That is, $|k, \alpha\rangle \equiv |x_1 \dots x_N\rangle$ and $\alpha = 1, \dots, l_k$, where l_k denotes the number of orthonormal states with the same irrep label k . In the basis $|k, \alpha\rangle$, the state $|\psi\rangle^{\otimes N}$ can be written

as

$$|\psi\rangle^{\otimes N} = \sum_{k=0}^{M-1} \sum_{\alpha=1}^{l_k} \sqrt{c_{k,\alpha}} |k, \alpha\rangle, \quad (36)$$

where $c_{k,\alpha}$ are of the form $c_{k,\alpha} = \prod_{j=0}^{M-1} p_j^{r_j}$, and r_j are positive integers (corresponding to the number of times $x_j \in (0, \dots, d-1)$ appears in $|k, \alpha\rangle$) satisfying $\sum_j r_j = N$ and $(\sum_j j r_j)_{\text{mod } M} = k$. Moreover, by \mathbb{Z}_M -invariant unitary operations we can transform

$$\frac{\sum_{\alpha} \sqrt{c_{k,\alpha}} |k, \alpha\rangle}{\sqrt{\sum_{\alpha} c_{k,\alpha}}}, \quad (37)$$

to the standard state $|k\rangle \in \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$. This transformation brings $|\psi\rangle^{\otimes N}$ to the form

$$|\psi\rangle^{\otimes N} = \sum_{k=0}^{M-1} \sqrt{c_k} |k\rangle, \quad (38)$$

where

$$c_k = \sum \binom{N}{r_0 \dots r_{M-1}} p_0^{r_0} \dots p_{M-1}^{r_{M-1}}, \quad (39)$$

are the multinomial coefficients that arise from the expansion $(\sum_k \sqrt{p_k} |k\rangle)^{\otimes N}$, where terms giving rise to the same irrep label k are grouped together. We note that the sum in Eq. (39) is taken over integers r_j for which $\sum_j r_j = N$ and $(\sum_j j r_j)_{\text{mod } M} = k$.

Note that Eq. (39) is similar to Eq. (12) in the $U(1)$ case above with the important difference that $\sum_j j r_j$ is modulo M . As we are considering finite cyclic groups $M \ll N$, and in the limit $N \rightarrow \infty$ the probability distribution $\{c_k\}$ can no longer be approximated with the normal distribution.

The coefficients c_k can also be written as

$$c_k = \sum_{m_1=0}^{M-1} \dots \sum_{m_N=0}^{M-1} \delta_{\bar{m}, k} p_{m_1} \dots p_{m_N}, \quad (40)$$

where $\bar{m} = \sum_i m_i$. In order to simplify calculations involving the discrete probability coefficients $\{c_k\}$, we use the discrete Fourier transform to re-write Eq. (40) as

$$c_k = \frac{1}{M} \sum_{n=0}^{M-1} e^{-\frac{i 2 \pi k n}{M}} z_n, \quad (41)$$

where

$$z_n \equiv \left(\sum_{m=0}^{M-1} e^{\frac{i 2 \pi n m}{M}} p_m \right)^N \equiv (r_n e^{i \theta_n})^N, \quad (42)$$

with $0 < r_n \leq 1$ and the phase $\theta_n \in [0, 2\pi)$. Since $z_0 = 1$, Eq. (41) can be written as

$$c_k = \frac{1}{M} \left(1 + \sum_{n=1}^{M-1} e^{-\frac{i 2 \pi k n}{M}} z_n \right) \equiv \frac{1}{M} (1 + \Delta_k), \quad (43)$$

where Δ_k must be real since c_k are real. Moreover, using the triangle inequality $|\Delta_k| \leq \sum_{n=1}^{M-1} |z_n|$. As $1 \leq n \leq M-1$, and $\sum_{m=0}^{M-1} p_m = 1$, where $p_m < 1$, $\forall m \in (0, \dots, M-1)$, there exists $0 < s_n < 1$ such that $|r_n e^{i\theta_n}| < s_n$. Therefore, $|z_n| < s_n^N$. Denoting $s_{\max} \equiv \max\{s_n\}$ it follows that $|\Delta_k| \leq (M-1)s_{\max}^N$, and in the limit $N \rightarrow \infty$, $|\Delta_k|$ goes exponentially to zero for all k , which also implies that as $N \rightarrow \infty$, $c_k \rightarrow 1/M$.

Indeed the set of states

$$\left\{ T(g) |+\rangle = \frac{1}{M} \sum_{k=0}^{M-1} e^{\frac{i2\pi k g}{M}} |k\rangle \mid g = 0, \dots, M-1 \right\}, \quad (44)$$

where $|+\rangle \equiv T(g=0) |+\rangle$, are optimal resources if Alice and Bob lack a shared frame of reference for \mathbb{Z}_M . Bob can perfectly distinguish the states in Eq. (44) and learn Alice's reference frame. For example, if Alice and Bob lack a chiral frame, associated with \mathbb{Z}_2 , then the states $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$, encode all the information about Alice's reference frame. If Bob detects $|+\rangle$ then he knows that his and Alice's chiral frames are aligned, else they are anti-aligned.

Bob's description of the N qudits sent to him by Alice is given by

$$|\psi(g)\rangle = (T(g) |\psi\rangle)^{\otimes N} = \sum_{k=0}^{M-1} \sqrt{c_k} e^{\frac{i2\pi k g}{M}} |k\rangle. \quad (45)$$

Due to the lack of a shared reference frame, Bob has complete ignorance about the element $g \in \mathbb{Z}_M$. As the superselection rule does not forbid us from performing any unitary on the multiplicity spaces, the state $|\psi(g)\rangle^{\otimes N}$ can be embedded in a M -dimensional Hilbert space. Bob's task is, therefore, to extract information about $g \in \mathbb{Z}_M$ from a state in an M -dimensional Hilbert space instead of a d^N -dimensional Hilbert space.

Suppose Bob's POVM is given by $\{E_y, y \in \mathbb{Z}_M\}$, where $E_y \geq 0$, with $\sum_{y \in \mathbb{Z}_M} E_y = I = \sum_{k=0}^{M-1} |k\rangle\langle k|$. We would like to quantify how much Bob learns about $g \in \mathbb{Z}_M$ from such a measurement. Denote by X the random variable associated with the relative group element, $x \in \mathbb{Z}_M$, between Alice's and Bob's reference frames. That is $X = x$ with uniform probability distribution $p_x = 1/M$. Denote also by Y the random variable associated with Bob's measurement outcome, $y \in \mathbb{Z}_M$. Using the same reasoning as in Sec. III A the accessible information per copy obeys

$$\frac{I_{\mathbb{Z}_M}^{(N)}(X : Y)}{N} \leq \frac{H(\{c_k\})}{N}. \quad (46)$$

where $H(\{c_k\})$ is the Shannon entropy of the probability distribution $\{c_k\}$. Using Eq. (43), the latter reads

$$H(\{c_k\}) = -\frac{1}{M} \sum_{k=0}^{M-1} (1 + \Delta_k) \log \left(\frac{1}{M} (1 + \Delta_k) \right). \quad (47)$$

As Δ_k are small, we can use the Taylor expansion for the logarithm. Thus, noting that $\sum_{k=0}^{M-1} \Delta_k = 0$, Eq. (47) can be written as

$$H(\{c_k\}) = \log M - \frac{1}{M \ln 2} \sum_{k=0}^{M-1} \sum_{n=2}^{\infty} (-1)^n \frac{\Delta_k^n}{n(n-1)}. \quad (48)$$

Note that $H(\{c_k\})$ is equal to $\log M$ with a correction that, for large N , goes exponentially to zero (recall that the Δ_k 's go exponentially to zero). We now find out the dominant part of this correction.

First, note that

$$\begin{aligned} \sum_k \Delta_k^2 &= \sum_{k=0}^{M-1} \sum_{n,m=1}^{M-1} e^{\frac{i2\pi k(n+m)}{M}} z_n z_m = M \sum_{n=1}^{M-1} |z_n|^2 \\ \sum_k \Delta_k^3 &= \sum_{k=0}^{M-1} \sum_{n,m,l=1}^{M-1} e^{\frac{i2\pi k(n+m+l)}{M}} z_n z_m z_l \\ &= M \sum_{n,m=1}^{M-1} z_n z_m z_{M-(m+n)}, \end{aligned} \quad (49)$$

and similar expressions can be found for $\sum_k \Delta_k^n$ for $n > 3$. Writing the complex numbers z_n as in Eq. (42), Eq. (49) becomes

$$\begin{aligned} \sum_k \Delta_k^2 &= M \sum_{n=1}^{M-1} r_n^{2N} \\ \sum_k \Delta_k^3 &= M \\ &\times \sum_{n,m=1}^{M-1} (r_n r_m r_{M-(m+n)})^N \cos(N(\theta_n + \theta_m + \theta_{M-(m+n)})). \end{aligned} \quad (50)$$

As the sums in Eq. (50) are over terms that are very small, we focus here only on the dominant terms with the maximum value of r_n . We therefore define

$$S = \{l \mid r_l = r_{\max}\} ; \quad r_{\max} \equiv \max_{n=1, \dots, M-1} \left| \sum_{m=0}^{M-1} e^{\frac{i2\pi n m}{M}} p_m \right|$$

to be the set of all integers, l , for which the magnitude of z_l (see Eq. (42)) is maximum.

While the dominant terms in the first sum of Eq. (50) are proportional to r_{\max}^{2N} , the second sum is exponentially smaller than r_{\max}^{2N} . Similarly, for any $n > 2$ the sum $\sum_k \Delta_k^n$ is exponentially smaller than r_{\max}^{2N} . Therefore, Eq. (48) can be written as

$$H(\{c_k\}) = \log M - r_{\max}^{2N} \left(\frac{|S|}{2 \ln 2} + O \left(\left(\frac{r}{r_{\max}} \right)^N \right) \right), \quad (51)$$

where r is some positive number smaller than r_{\max} , and $|S|$ denotes the size of S . Note that the maximum

$H(\{c_k\})$ can be $\log M$, and this maximum is achieved if and only if $|\psi\rangle$ in Eq. (35) is one of the optimal resource states in Eq. (44). It follows that the regularized \mathbb{Z}_M -asymmetry goes to zero in the limit $N \rightarrow \infty$.

Just as in the $U(1)$ case we need to modify the \mathbb{Z}_M -asymmetry so that it scales linearly in N . This is achieved by defining the linearization function, $\mathcal{L} : \mathcal{R} \rightarrow \mathcal{R}$ to be [25]

$$\mathcal{L}(x) = -\log(\log M - x).$$

As this is a monotonically increasing function it follows that

$$\frac{\mathcal{L}(I_{\mathbb{Z}_M}^{(N)}(X : Y))}{N} \leq \frac{\mathcal{L}(A_{\mathbb{Z}_M}((|\psi\rangle\langle\psi|)^{\otimes N}))}{N}. \quad (52)$$

In the following theorem we show that in the limit $N \rightarrow \infty$, the inequality in Eq. (52) is saturated.

Theorem 2 Let $|\psi\rangle = \sum_{k=0}^{M-1} \sqrt{p_k} |k\rangle$ as in Eq. (35). Then, for $G = \mathbb{Z}_M$

$$R_G(\psi) = A_G^{(reg)}(\psi) = -2 \log r_{\max},$$

where

$$r_{\max} = \max_{n \in \{1, 2, \dots, M-1\}} \left| \sum_{m=0}^{M-1} e^{\frac{i 2 \pi n m}{M}} p_m \right|$$

Proof. Let Bob's POVM elements be given by $E_y = |e_y\rangle\langle e_y|$, where

$$|e(y)\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} e^{\frac{i 2 \pi k y}{M}} |k\rangle. \quad (53)$$

Note that $\sum_{y \in \mathbb{Z}_M} E_y = I = \sum_{k=0}^{M-1} |k\rangle\langle k|$. We will show that the measurement in Eq. (53) maximizes $H^{(N)}(X : Y)$ given by

$$H^{(N)}(X : Y) = \sum_{x,y} p(x,y) \log \left(\frac{p(x,y)}{p(x)p(y)} \right), \quad (54)$$

where the joint probability distribution $p(x,y)$ can be calculated using Bayes' rule $p(x,y) = p(y|x)p(x)$, and

$$\begin{aligned} p(x) &= \frac{1}{M} \\ p(y|x) &= |\langle e(y)|\psi(x)\rangle|^2 \end{aligned} \quad (55)$$

Substituting Eqs. (45,53) into Eq. (55) gives

$$\begin{aligned} p(y|x) &= \frac{1}{M} \sum_{k,l=0}^{M-1} \sqrt{c_k c_l} e^{\frac{i 2 \pi (k-l)(x-y)}{M}} \\ &= \frac{1}{M} \left| \sum_{k=0}^{M-1} \sqrt{c_k} e^{\frac{i 2 \pi k(x-y)}{M}} \right|^2 \end{aligned} \quad (56)$$

From the equation above we see that $p(y|x) = p(x|y)$. Therefore, the probability that $Y = y$ is given by

$$p(y) = \sum_{x=0}^{M-1} p(y|x)p(x) = \frac{1}{M} \sum_{x=0}^{M-1} p(y|x) = \frac{1}{M}. \quad (57)$$

Hence, Eq. (54) reduces to

$$H^{(N)}(X : Y) = \log M + \frac{1}{M} \sum_{x,y=0}^{M-1} p(y|x) \log(p(y|x)), \quad (58)$$

and using Eq. (43) the conditional probabilities, $p(y|x)$, maybe written as

$$p(y|x) = \frac{1}{M^2} \sum_{k,l=0}^{M-1} e^{\frac{i 2 \pi (k-l)(x-y)}{M}} \sqrt{(1 + \epsilon_{kl})}, \quad (59)$$

where $\epsilon_{kl} = \Delta_k + \Delta_l + 2\Delta_k \Delta_l$. As ϵ_{kl} is small and second order in Δ , expanding the square root in Eq. (59) to second order in ϵ_{kl} gives

$$\begin{aligned} p(y|x) &= \frac{1}{M^2} \sum_{k,l=0}^{M-1} e^{\frac{i 2 \pi (k-l)(x-y)}{M}} \left(1 + \frac{1}{2}(\Delta_k + \Delta_l) \right. \\ &\quad \left. - \frac{1}{8}(\Delta_k^2 + \Delta_l^2) + \frac{1}{4}\Delta_k \Delta_l \right) + O(\epsilon_{kl}^3). \end{aligned} \quad (60)$$

As $p(y|x) = p(x|y)$, and $\sum_{k=0}^{M-1} \Delta_k = 0$,

$$\frac{1}{4M^2} \sum_{k,l=0}^{M-1} e^{\frac{i 2 \pi (x-y)(k-l)}{M}} \Delta_k \Delta_l = \begin{cases} 0 & \text{if } x = y \\ \frac{1}{4}|z_{x-y}|^2 & \text{if } x \neq y \end{cases}, \quad (61)$$

and Eq. (60) can be written, after some algebra, as

$$\begin{aligned} p(x|x) &= 1 - \frac{1}{4M} \sum_{k=0}^{M-1} \Delta_k^2 + O(\Delta_k^3) \\ p(y \neq x|x) &= \frac{1}{4}|z_{x-y}|^2. \end{aligned} \quad (62)$$

Using the same arguments as in Eqs. (48-51) above, Eq. (62) can be written as

$$\begin{aligned} p(x|x) &= 1 - \frac{r_{\max}^{2N}}{4} \left(|S| + O\left(\left(\frac{r}{r_{\max}} \right)^N \right) \right) \\ p(y \neq x|x) &= \frac{1}{4}|z_{x-y}|^2. \end{aligned} \quad (63)$$

We now break the mutual information, Eq. (58), into two terms

$$\begin{aligned} H^{(N)}(X : Y) &= \log M + \frac{1}{M} \sum_{x=0}^{M-1} p(x|x) \log(p(x|x)) \\ &\quad + \frac{2}{M} \sum_{x>y} p(y|x) \log(p(y|x)) \end{aligned} \quad (64)$$

Using Eq. (63), the approximation $(1-x)\log(1-x) = \frac{1}{\ln 2}(-x + O(x^2))$, and noting that the terms in the first sum of Eq. (64) are independent of x , we obtain

$$\begin{aligned} & \frac{1}{M} \sum_{x=0}^{M-1} p(x|x) \log p(x|x) \\ &= -\frac{r_{\max}^{2N}}{4 \ln 2} \left(|S| + O\left(\left(\frac{r}{r_{\max}}\right)^N\right) \right). \end{aligned} \quad (65)$$

The second sum in Eq. (64) reads

$$\frac{2}{M} \sum_{x>y} p(y|x) \log(p(y|x)) = \frac{1}{2M} \sum_{x>y} |z_{x-y}|^2 \log\left(\frac{|z_{x-y}|^2}{4}\right). \quad (66)$$

Denoting $n = x - y$ and noting that $\sum_{x>y} = \sum_{n=1}^{M-1} \sum_{y=0}^{M-1-n}$, Eq. (66) becomes

$$\begin{aligned} & \frac{2}{M} \sum_{x>y} p(y|x) \log(p(y|x)) = \\ & \frac{1}{2M} \sum_{n=1}^{M-1} (M-n) |z_n|^2 (\log |z_n|^2 - 2). \end{aligned} \quad (67)$$

Plugging Eqs. (65, 67) into Eq. (64) gives

$$\begin{aligned} H^{(N)}(X : Y) &= \log M - \frac{r_{\max}^{2N}}{4 \ln 2} \left(|S| + O\left(\left(\frac{r}{r_{\max}}\right)^N\right) \right) \\ &+ \frac{1}{2M} \sum_{n=1}^{M-1} (M-n) |z_n|^2 (\log |z_n|^2 - 2). \end{aligned} \quad (68)$$

As only the largest $|z_n|$'s will contribute significantly to the mutual information, Eq. (68) reduces to

$$\begin{aligned} H^{(N)}(X : Y) &= \log M - r_{\max}^{2N} \left(\frac{|S|}{4 \ln 2} + \frac{1}{M} \sum_{s \in S} (M-s) \right. \\ &\quad \left. + \frac{N \log(r_{\max})}{M} \sum_{s \in S} (M-s) + O\left(\left(\frac{r}{r_{\max}}\right)^N\right) \right), \end{aligned} \quad (69)$$

Denoting by $D \equiv \frac{\sum_{s \in S} (M-s)}{M}$, Eq. (69) becomes

$$\begin{aligned} H^{(N)}(X : Y) &= \log M \\ &- r_{\max}^{2N} \left(\frac{|S|}{4 \ln 2} + D(1 - N \log r_{\max}) + O\left(\left(\frac{r}{r_{\max}}\right)^N\right) \right) \end{aligned} \quad (70)$$

Finally, linearizing both the mutual information and

the \mathbb{Z}_M -asymmetry yields

$$\begin{aligned} \mathcal{L}(A_{\mathbb{Z}_M}((|\psi\rangle\langle\psi|)^{\otimes N})) &= -\log\left(\frac{|S|}{2 \ln 2} + O\left(\left(\frac{r}{r_{\max}}\right)^N\right)\right) \\ &- 2N \log r_{\max} \\ \mathcal{L}(H^{(N)}(X : Y)) &= -\log\left(\frac{|S|}{4 \ln 2} + D(1 - N \log r_{\max}) \right. \\ &\quad \left. + O\left(\left(\frac{r}{r_{\max}}\right)^N\right)\right) - 2N \log r_{\max}. \end{aligned} \quad (71)$$

Dividing both quantities in Eq. (71) by N and taking the limit $N \rightarrow \infty$, one notes that the first term in both quantities tends to zero. Thus

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{\mathcal{L}(A_{\mathbb{Z}_M}((|\psi\rangle\langle\psi|)^{\otimes N}))}{N} &= \lim_{N \rightarrow \infty} \frac{\mathcal{L}(H^{(N)}(X : Y))}{N} \\ &= -2 \log r_{\max} \end{aligned} \quad (72)$$

This completes the proof. \square

Thus the alignment rate is equal to the regularized, linearized \mathbb{Z}_M -asymmetry. In the next section we show, somewhat surprisingly, that the additivity of $R_G(\psi)$ does not hold for all finite abelian groups.

IV. SUPERADDITIVITY OF $R_G(\psi)$

The G -asymmetry given in Eq. (1) is an ensemble frameness monotone [4, 6], i.e. it does not increase on average under G -invariant operations. However, the regularized, linearized G -asymmetry, $A_G^{(reg)}$ (see Eq.(5)), is not necessarily an ensemble monotone (as was shown for the case where $G = \mathbb{Z}_2$ in [4]). Nonetheless, as the linearization function is monotonically increasing, $A_G^{(reg)}$ must be a deterministic frameness monotone. That is, $A_G^{(reg)}$, does not increase under deterministic G -invariant operations (see [4] for more details). As such $A_G^{(reg)}$ quantifies how well a quantum state can serve as a token of the missing reference frame.

In addition, from its definition, $A_G^{(reg)}$ is weakly additive; i.e. $A_G^{(reg)}(\psi^{\otimes 2}) = 2A_G^{(reg)}(\psi)$. As $R_G(\psi) = A_G^{(reg)}(\psi)$ for $G = U(1)$ and $G = \mathbb{Z}_M$, it follows that $R_G(\psi)$ (for $G = U(1)$ or $G = \mathbb{Z}_M$) is also a deterministic frameness monotone that is weakly additive as one would intuitively expect. The question we address in this section is whether R_G is also strongly additive; that is, for any two pure states $|\psi\rangle$ and $|\phi\rangle$ is it true that

$$R_G(\psi \otimes \phi) = R_G(\psi) + R_G(\phi) ? \quad (73)$$

In the case where $G = U(1)$ Eq. (73) is true. Indeed, we have seen in the previous section that for $G = U(1)$, the alignment rate $R_{U(1)}(\psi) = 4\pi V(\psi)$, where $V(\psi)$ is

the variance of the state $|\psi\rangle$. It was shown in [4] that the variance is strongly additive as $V(\psi \otimes \phi) = V(\psi) + V(\phi)$ for any two states $|\psi\rangle, |\phi\rangle$. Note that $R_{U(1)}(\psi)$ is strongly additive because it is equal to the variance. One cannot infer the strong additivity of $R_{U(1)}(\psi)$ from its definition without the explicit calculation of the previous section.

In the resource theory of pure bipartite entanglement, a similar situation occurs. The *entanglement cost* is defined as the rate at which one can convert, by local means, many copies of pure bipartite singlets to many copies of another bipartite state ρ^{AB} (which we will call the target state). Therefore, by definition, the entanglement cost is weakly additive under tensor product of the same bipartite state. If the target state is a *pure* bipartite state, then the entanglement cost rate is given by the *entropy of entanglement*. Since the latter is defined as the von-Neuman entropy of the reduced density matrix $\text{Tr}_B |\psi^{AB}\rangle\langle\psi^{AB}|$, it follows that the entanglement cost rate is also strongly additive in the case of pure bipartite states. Moreover, it was believed for quite sometime that the entanglement cost is also strongly additive under tensor product of two *mixed* bipartite states. Remarkably, this (somewhat intuitive) additivity conjecture was proved to be false in a recent paper by Hastings [24].

It is therefore natural to ask if R_G is also additive under tensor product of two distinct *mixed* states. In this paper, however, we will not try to answer this question. Instead, we now show that for some groups, R_G is not strongly additive even under the tensor product of two (distinct) *pure* states.

Suppose Alice and Bob lack a shared frame of reference associated with the group \mathbb{Z}_M . Consider two resource states (or bounded-size quantum reference frames [2]) $|\psi\rangle = \sum_{k=0}^{M-1} \sqrt{p_k} |k\rangle$ and $|\phi\rangle = \sum_{k=0}^{M-1} \sqrt{q_k} |k\rangle$ (these resource states serve as a token for the missing reference frame). From Theorem 2 we have

$$R_{\mathbb{Z}_M}(|\psi\rangle) = -2 \log r_{\max} \quad \text{and} \quad R_{\mathbb{Z}_M}(|\phi\rangle) = -2 \log l_{\max}$$

where

$$r_{\max} = \max_{n \in \{1, \dots, M-1\}} \left| \sum_{m=0}^{M-1} e^{\frac{i2\pi n m}{M}} p_m \right|$$

$$l_{\max} = \max_{n \in \{1, \dots, M-1\}} \left| \sum_{m=0}^{M-1} e^{\frac{i2\pi n m}{M}} q_m \right|.$$

We now calculate $R_{\mathbb{Z}_M}(|\psi\rangle \otimes |\phi\rangle)$. Up to \mathbb{Z}_M -invariant unitaries, $|\psi\rangle \otimes |\phi\rangle$ can be written as

$$|\psi\rangle \otimes |\phi\rangle = \sum_{k_1, k_2=0}^{M-1} \sqrt{p_{k_1} q_{k_2}} |k_1\rangle \otimes |k_2\rangle = \sum_k \sqrt{c_k} |k\rangle, \quad (74)$$

where $c_k = \sum p_{k_1} q_{k_2}$, and the sum is over all k_1, k_2 such that $k_1 + k_2 = k \pmod{M}$. Computing the Fourier transform

of the coefficients c_k , one obtains

$$\omega_n = \sum_{m=0}^{M-1} e^{\frac{i2\pi n m}{M}} c_m = \sum_{m=0}^{M-1} \sum_{k_1+k_2=m} e^{\frac{i2\pi n (k_1+k_2)}{M}} p_{k_1} q_{k_2}. \quad (75)$$

Noting that $\sum_{m=0}^{M-1} \sum_{k_1+k_2=m} = \sum_{k_1=0}^{M-1} \sum_{k_2=0}^{M-1}$, Eq. (75) reduces to

$$\omega_n = \sum_{k_1=0}^{M-1} e^{\frac{i2\pi k_1 n}{M}} p_{k_1} \sum_{k_2=0}^{M-1} e^{\frac{i2\pi k_2 n}{M}} q_{k_2} \equiv r_n l_n e^{i(\theta_n + \phi_n)}, \quad (76)$$

where r_n and l_n are the absolute values of the Fourier transforms of $\{p_k\}$ and $\{q_k\}$, respectively. We therefore get

$$\begin{aligned} R_{\mathbb{Z}_M}(\psi \otimes \phi) &= \max_{n \in \{1, \dots, M-1\}} (-2 \log r_n - 2 \log l_n) \\ &\geq -2 \log r_{\max} - 2 \log l_{\max} \\ &= R_{\mathbb{Z}_M}(\psi) + R_{\mathbb{Z}_M}(\phi). \end{aligned} \quad (77)$$

Hence, $R_{\mathbb{Z}_M}$ is not strongly additive in general. For the case where $M = 2$, $R_{\mathbb{Z}_M}$ is strongly additive since there is only a single n , namely $n = 1$. For the case where $M = 3$, $R_{\mathbb{Z}_M}$ is again strongly additive as there are only two values for n , which turn out to satisfy $\omega_1 = \omega_2^*$ and thus $|\omega_1| = |\omega_2|$. However, for $M \geq 4$, $R_{\mathbb{Z}_M}$ is super-additive as the following example shows.

Consider the case where Alice and Bob lack a shared frame of reference for \mathbb{Z}_4 and Alice has the states

$$\begin{aligned} |\psi\rangle &= \sqrt{\frac{13}{64}} |0\rangle + \sqrt{\frac{18}{64}} |1\rangle + \sqrt{\frac{19}{64}} |2\rangle + \sqrt{\frac{14}{64}} |3\rangle \\ |\phi\rangle &= \sqrt{\frac{7}{20}} |0\rangle + \sqrt{\frac{3}{20}} |1\rangle + \sqrt{\frac{6}{20}} |2\rangle + \sqrt{\frac{4}{20}} |3\rangle. \end{aligned} \quad (78)$$

Computing the Fourier transforms one obtains $r_1 = r_3 = 0.113$, $r_2 = 0$, and $l_1 = l_3 = 0.07$, $l_2 = 0.3$. Thus, $r_{\max} = r_1 = 0.113$, and $l_{\max} = l_2 = 0.3$. Moreover, $|\omega_1| = 0.008$, $|\omega_2| = 0$ and $|\omega_3| = 0.008$. We therefore have $|\omega_{\max}| = r_1 l_1$ which is smaller than $r_{\max} l_{\max}$. Thus, $R_{\mathbb{Z}_4}(|\psi\rangle \otimes |\phi\rangle)$ is strictly greater than $R_{\mathbb{Z}_4}(|\psi\rangle) + R_{\mathbb{Z}_4}(|\phi\rangle)$.

In order to understand the meaning of the super-additivity of R_G , suppose that Bob holds many copies of two resource states $|\psi\rangle$ and $|\phi\rangle$. In particular, consider the state $|\psi\rangle^{\otimes N} \otimes |\phi\rangle^{\otimes N}$, where $N \gg 1$. In order to learn Alice's reference frame, Bob performs measurements on the resource states sent to him by Alice. The super-additivity of R_G indicates that in order for Bob to learn the most about Alice's reference frame, he should perform a joint measurement on the full system $|\psi\rangle^{\otimes N} \otimes |\phi\rangle^{\otimes N}$, rather than two separate joint measurements, one on $|\psi\rangle^{\otimes N}$ and the other on $|\phi\rangle^{\otimes N}$.

V. CONCLUSION

To summarize, we have derived an information-theoretic, operational interpretation for the G -asymmetry

for the case of a phase reference, and a reference frame associated with a discrete cyclic group of M elements, \mathbb{Z}_M . In particular, we have shown that the alignment rate, $R_G(\psi)$, in a phase alignment protocol associated with $G = U(1)$, and an alignment protocol associated with a finite cyclic group of order M , \mathbb{Z}_M , is equal to the regularized, linearized G -asymmetry, $A_G^{\text{reg}}(\psi)$. As the G -asymmetry is equal to the Holevo bound, our result implies that for reference frames associated with $G = U(1)$ and $G = \mathbb{Z}_M$, the linearized Holevo bound is asymptotically achievable. We are willing to conjecture that $R_G = A_G^{\text{reg}}$ for all finite or compact Lie groups.

The additivity of $R_G(\psi)$ was discussed in Sec. IV, where it was shown that $R_G(\psi)$ is both weakly and strongly additive for $G = U(1)$, $G = \mathbb{Z}_2$, and $G = \mathbb{Z}_3$, but only weakly additive for finite cyclic groups, \mathbb{Z}_M , for $M \geq 4$. For the latter, we proved that R_G is super-additive. In the case of finite groups however, there exists a resource state, denoted here by $|+\rangle$, which *completely* elevates the restrictions that follow from the lack of a shared reference frame. It is therefore the ultimate resource Bob can hold. It turns out that up to \mathbb{Z}_M -invariant unitary operations, $|\psi\rangle^{\otimes N}$ approaches the ultimate resource state $|+\rangle$

in the limit $N \rightarrow \infty$. Hence, it follows from Eq.(51) for example, that the super-additivity of $R_{\mathbb{Z}_M}(\psi)$ indicates only an exponentially small gain of reference-frame information in the performance of a joint measurement on the full system, $|\psi\rangle^{\otimes N} \otimes |\phi\rangle^{\otimes N}$, rather than two separate joint measurements on $|\psi\rangle^{\otimes N}$ and $|\phi\rangle^{\otimes N}$. It is therefore left open if there are non-finite compact Lie groups for which R_G is super-additive. Such examples, if exist, will have a more significant gain (i.e. not exponentially small) of reference-frame information in the performance of a joint measurement on the full system, $|\psi\rangle^{\otimes N} \otimes |\phi\rangle^{\otimes N}$, rather than two separate joint measurements on $|\psi\rangle^{\otimes N}$ and $|\phi\rangle^{\otimes N}$.

VI. ACKNOWLEDGEMENTS

We are grateful to Fernando Brandão, Giulio Chiribella, Iman Marvian, Aram W. Harrow, and Robert W. Spekkens for helpful discussions on this work. We gratefully acknowledge support from NSERC and USARO.

-
- [1] S. D. Bartlett and H. M. Wiseman. Entanglement constrained by superselection rules. *Phys. Rev. Lett.*, 91(9):097903, 2003.
 - [2] S. D. Bartlett, T. Rudolph, R. W. Spekkens, and P. S. Turner. Quantum communication using a bounded-size quantum reference frame. *New Journal of Physics*, 11(6):063013, 2009.
 - [3] A. Peres and P. F. Scudo. Transmission of a cartesian frame by a quantum system. *Phys. Rev. Lett.*, 87(16):167901, Sep 2001.
 - [4] G. Gour and R. W. Spekkens. The resource theory of quantum reference frames: manipulations and monotones. *New Journal of Physics*, 10(3):033023, 2008.
 - [5] M. Marvian and R. W. Spekkens, 2011. arXiv:1105.1816v1; arXiv:1104.0018v1.
 - [6] G. Gour, I. Marvian, and R. W. Spekkens. Measuring the quality of a quantum reference frame: The relative entropy of frameness. *Phys. Rev. A*, 80(1):012307, Jul 2009.
 - [7] B. Toloui, G. Gour, and B. C. Sanders, 2011. arXiv:1104.1144v1.
 - [8] J. A. Vaccaro, F. Anselmi, H. M. Wiseman, and K. Jacobs. Tradeoff between extractable mechanical work, accessible entanglement, and ability to act as a reference system, under arbitrary superselection rules. *Phys. Rev. A*, 77(3):032114, Mar 2008.
 - [9] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57(3):1619–1633, Mar 1998.
 - [10] E. Bagan, M. Baig, A. Brey, R. Muñoz-Tapia, and R. Tarrach. Optimal strategies for sending information through a quantum channel. *Phys. Rev. Lett.*, 85(24):5230–5233, Dec 2000.
 - [11] A. Peres and P. F. Scudo. Entangled quantum states as direction indicators. *Phys. Rev. Lett.*, 86(18):4160–4162, Apr 2001.
 - [12] E. Bagan, M. Baig, A. Brey, R. Muñoz-Tapia, and R. Tarrach. Optimal encoding and decoding of a spin direction. *Phys. Rev. A*, 63(5):052309, Apr 2001.
 - [13] E. Bagan, M. Baig, and R. Muñoz-Tapia. Aligning reference frames with quantum states. *Phys. Rev. Lett.*, 87(25):257903, Nov 2001.
 - [14] E. Bagan, M. Baig, and R. Muñoz-Tapia. Quantum reverse engineering and reference-frame alignment without nonlocal correlations. *Phys. Rev. A*, 70(3):030301, Sep 2004.
 - [15] G. Chiribella, G. M. D’Ariano, P. Perinotti, and M. F. Sacchi. Efficient use of quantum resources for the transmission of a reference frame. *Phys. Rev. Lett.*, 93(18):180503, Oct 2004.
 - [16] J. von Korff and J. Kempe. Quantum advantage in transmitting a permutation. *Phys. Rev. Lett.*, 93(26):260502, Dec 2004.
 - [17] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.*, 79(2):555–609, Apr 2007.
 - [18] A. S. Holevo. Statistical problems in quantum physics. In G. Maruyama and Yu. Prokhorov, editors, *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, volume 330 of *Lecture Notes in Mathematics*, pages 104–119. Springer Berlin / Heidelberg, 1973. 10.1007/BFb0061483.
 - [19] M. Horodecki, J. Oppenheim, and R. Horodecki. Are the laws of entanglement theory thermodynamical? *Phys. Rev. Lett.*, 89(24):240403, Nov 2002.
 - [20] S. Sternberg. *Group Theory and Physics*. Cambridge University Press, 1994.
 - [21] N. Schuch, F. Verstraete, and J. I. Cirac. Quantum en-

- tanglement theory in the presence of superselection rules. *Phys. Rev. A*, 70(4):042310, Oct 2004.
- [22] R. Durrett. *Probability Theory and Examples*. Cambridge University Press, New York, 2010.
- [23] G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi. Covariant quantum measurements that maximize the likelihood. *Phys. Rev. A*, 70(6):062105, Dec 2004.
- [24] M. B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nat Phys*, 5(4):255–257, 04 2009.
- [25] Following the linearization introduced in [4] for the special case of $G = \mathbb{Z}_2$.